CSIS

Anthony H. Cordesman
Arleigh A. Burke Chair in Strategy
Center for Strategic and International Studies
1800 K Street N.W.
Suite 400
Washington, D.C. 20006
(202) 775-3270
Acordesman@aol.com

The Changing Face of Terrorism and Technology, and the Challenge of Asymmetric Warfare

Testimony to the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information

Anthony H. Cordesman

March 27, 2001

"Terrorism" is a topic that arouses so much fear and revulsion that there is a natural tendency to "cry wolf," and to confuse the potential threat with one that is actually occurring. Similarly, any discussion of the new threats posed by weapons of mass destruction and information warfare involves threats that are so serious that there is an equal tendency to respond like Chicken Little and worry that the sky is falling.

This scarcely means we should not be worried about terrorism. The potential threats to our society are all too real. Democratic societies are inherently vulnerable. They place few controls over their borders, their citizens, or foreigners who have actually entered their territory. This is particularly true of the US, and there are many vulnerable points in our social structure and economy that foreign governments and extremist movements, domestic extremists and the mentally ill can attack.

There equally are good reasons to be increasingly concerned about new forms of asymmetric warfare and terrorism, and the use of new and more lethal forms of technology.

Yet, there are equally good reasons to be careful about exaggerating the threat, and being careless about the way we define it. We can improve intelligence, defense, and response in many ways. We can anticipate future risks, even if we cannot predict the future. We do, however, have limited resources and competing priorities, and we face daunting uncertainties about the nature of the problem terrorism poses to our security.

Crying Wolf Meets Chicken Little

It is not easy to characterize the threat – at least in unclassified terms. There are grave weaknesses and shortcomings in the statistics that the US government makes publicly available on terrorism. We do not have an adequate picture of the number, type, and seriousness of domestic incidents, and it is often difficult to separate out criminal activity, threats, actual action by domestic terrorists, and the actions of mentally disturbed individuals.

The data the US government publishes on international terrorist activity also has many defects. Much of it is highly over-aggregated, and does not provided anything approaching sophisticated pattern analysis. We stress international terrorism, but ignore largely foreign domestic violence that may generate terrorism in the future. We tend to demonize known terrorist groups, but ignore or underplay the capability of foreign states to conduct covert operations or use proxies to do so.

We exaggerate the existence of foreign networks, such as Usama Bin Ladin, and understate the risk that individual terrorist elements may lash out against us in ways we do not expect. Much of our analysis is grossly ethnocentric: It assumes that we are the key target of attacks which generally grow out of theater tensions and conflicts where we become a target – if at all – because of our ties to allies and peacekeeping missions.

The fact is, however, that if one looks at the recent patterns in terrorism, the US is no more subject to such attacks today – whether measured in numbers of incidents or casualties – than in the past. The net threat also remains a small one in actuarial terms. The word "terrorism" may trigger a great emotional reaction, but actual casualties and losses are almost actuarially insignificant. Far more people die of traffic accidents on a bad weekend than dies annually of terrorism.

The idea that the end of the Cold War has somehow created a more unstable and violent world is a myth. The world is, has always been, and will remain a violent place. According to the Department of Defense, there have been some 20-30 serious regional conflicts and civil wars going on every day of every year since the end of World War II. We did indeed relate many of these conflicts to the Cold War while it was going on, but in truth, most such conflicts dragged in the superpowers and were not caused by them.

With the exception of the Balkans, we do not see new major regional patterns of violence we can relate to the Cold War. In fact, the end of the Cold War has simply allowed us to focus on the broad realities of ongoing global violence rather than a single threat.

We need to be equally careful about exaggerating the new trends in technological vulnerability. Some of these trends are very real, but our critical infrastructure has always been vulnerable. Nature and chance have shown that repeatedly, and studies done back in the 1950s and 1960s showed how limited attacks – then postulated to be by attackers like the Soviet Spetsnaz – could cripple our utilities, paralyze critical military installations, or destroy our continuity of government. We have always been vulnerable to a truly well-organized terrorist or covert attack.

The fact that there are real wolves in the world, and that the sky can fall – at least – to the extent that far more serious damage is possible than we have ever suffered from in the past – is not a reason to cry wolf or play the role of chicken little.

The Changing Face of Terrorism and Technology

In saying this, I am all too well aware that no victim of terrorism, or their loved ones, are going to be consoled by the fact that they are a relatively small statistic. The political symbolism of successful terrorist attacks is also often far greater than the casualties, and even an empty threat can help to undermine the fabric of social trust upon which our democracy is based.

Equally important, the fact we have not yet encountered an attack in the US as serious as the strikes on our Embassies in Kenya and Tanzania, or as potentially threatening as Aum Shinrikyo, is in no way a guarantee for the future. Rather than exaggerate current threats, we need to be very conscious of the fact that the nature and seriousness of the threat can change suddenly and with little warning.

Let me give some specific examples:

- **At present the US government focuses most of its intelligence analysis, defense planning and response, around a relatively narrow definition of terrorism.** It focuses on independent terrorist groups, and not on the threat states can pose in asymmetric warfare. Yet, it is states that have the most access to weapons of mass destruction – particularly biological and nuclear weapons – and which have the most capability to launch sophistication attacks on our information systems.

We face current potential threats from nations like Iran, Iraq, Libya, and North Korea. We can face new threats as a result of our regional alliances and commitments every time a major conflict, crisis, or peace-keeping activity takes place.

Acts can come in the context of over asymmetric warfare, covert state-launched attacks, or the use of terrorist and extremist groups as proxies. Attacks can be made on our allies, our forces and facilities overseas, on US economic interests, or on our own territory. They can involve attackers with very different values, escalation ladders and perceptions and who lash out in a crisis.

This is also one area where the world has really changed since the end of the Cold War. We have always been a natural target because of the sheer scale of our global commitments and interest. Now, however, there is no Soviet Union our potential opponents can turn to, and they have no way of offsetting our advantage in conventional warfare.

We need to bridge the gap between the way in which the US government prepares for asymmetric warfare and to deal with the threat of terrorism -- not only in terms of intelligence analysis, but our defense and response planning for Homeland Defense. We also must include intelligence analysis of capabilities and not just intentions. History shows us that the fact that foreign countries and leaders are deterred, or show restraint today, is no guarantee they will behave the same way under crisis conditions.

We need to ensure the effective fusion of intelligence community efforts, military planning, and civil defense and response planning. We should not leave any gap where the Department of Defense seriously plans for large-scale nuclear and biological attacks and civil Departments and Agencies focus on relatively low-level conventional explosives and limited chemical attacks.

We need to be equally careful not to compartment our analysis of information warfare so that the Department worries about true information warfare while civil departments and agencies worry about hacking and cracking at much lower levels of threat.

Finally, we need to consider the full implications of our call for missile defense, and of our counterproliferation activities. The more we succeed in blocking overt threats, the more we will drive states towards finding alternative means of attack. It makes little sense to close the barn door and leave the windows open.

We need to focus on key areas of technological change. We cannot yet predict what technical capabilities hostile states, extremists and movements will acquire over the next 15-25 years. We can, however, predict that there are several major areas of technological change that can radically alter the effectiveness of asymmetric and terrorist attacks and which require care attention from the intelligence community:

- *The vulnerability of our critical infrastructure is changing*: Our financial systems, communications systems, utilities, and transportation nets are far more tightly integrated than in the past, and we rely far more on national and regional systems, rather than large autonomous local ones. This reduces vulnerability in some ways, but increases vulnerability in others. Systems netting and integration involves shifts in technology that need careful examination.

- *Information systems create new vulnerabilities*: It is all too possible to grossly over-exaggerate our dependency on information systems, their vulnerability, and the difficulty in finding work-arounds, and reconstituting critical systems. Many statements are being made that have no real analytic underpinning and the importance of given systems is poorly researched. The Internet, in particular, is being glamorized to the point of absurdity. Nevertheless, information systems have become part of our critical infrastructure, and virtually invisible cyberattacks may prove to be more lethal in some cases than high explosives. New physical methods of attack, such as EMP weapons, may also be becoming more practical.

- *Chemical weapons and toxins are changing*: It is impossible to discuss fourth generation chemical weapons in an unclassified forum, but the threat has been openly raised by Department of Defense officials. The technology and equipment for older types of chemical weapons is also proliferating at a civil level and becoming steadily more available to governments, extremist movements, and individuals.

- *Biological weapons are changing*: It has been possible to make dry storable biological weapons with nuclear lethality since at least the late 1950s. Advances in biotechnology, food processing equipment, pharmaceuticals, and other dual-use facilities and technologies are also proliferating at a civil level and becoming steadily more available to governments, extremist movements, and individuals. These problems are compound by the rapid spread of expertise and equipment for genetic engineering. The end result is that the technology of attacks on humans, livestock, and crops is becoming steadily more available, and in forms which not only can be extremely lethal and/or costly, but difficult to attribute to a given attacker.

- *The availability of nuclear weapons may change:* It is far too soon to say that broad changes are taking place in the nuclear threat. Nevertheless, the break up of the FSU, and proliferation in India and Pakistan, does create a growing risk that fissile material may become more available for “dirty” and low yield weapons, and the knowledge of how to make crude nuclear devices, handle the high explosives, provide neutron initiators, and deal with the complex triggering problems is also spreading.

- *The risk from radiological weapons may change:* Radiological weapons have not been particularly attractive options in the past. There is, however, a steadily growing mass of nuclear waste, and some studies indicate that the long-term genetic effects of such weapons may be more serious than their short-term effects.

- *The ability to exploit the media and psychological dimension of new technologies has grown:* Far more is involved than body counts, physical damage, and economic loss. Even the most limited CBRN or information attack on the US or US targets has great political and psychological impact both within the US and overseas. The spread of mass communications, and use of tools like the Internet and Satellite TV, also increases the impact of attacks.

It is all too easy to exaggerate today's threat in each of these areas, but it is equally easy to exaggerate the difficulties that individual terrorist movements and extremists now face in using such technologies. There is a clear need to examine how states can use such weapons covertly or through proxies, and forecast how widely spread each of these threats is likely to become in the future.

We need to reexamine the problem of vulnerability. We cannot hope to accurate predict our attacker or their means of attack, but we can do much to improve our analysis of vulnerability and shape our intelligence and planning effort around the need to detect threats to our greatest vulnerabilities. To be specific, there are several areas of vulnerability that need special attention:

- *We need to conduct and systematically update our analysis of the vulnerability of our critical infrastructure*, including financial systems, information systems, communications systems, utilities, and transportation nets and make sure our intelligence can focus on potential threats.
- *We need to reexamine our vulnerability to the chemical threat* in the light of fourth generation weapons, and the growing ease with which states, extremists, and terrorists can obtain them.
- *We need to rethink the risk of biological attack:* We need to look beyond the risk of the limited use of crude, long-known weapons and toxins, and assess the extent to which genetic weapons are increasing our vulnerabilities. We also need to look beyond single agent non-infectious attacks on human beings, and consider multiple agent attacks, infectious attacks, and/or attacks on our agriculture.
- *We need to reconsider the cumulative risk of covert or terrorist nuclear attack:* It still seems unlikely that any state or terrorist movement could both acquire a nuclear device in the near future, and be willing to take the risk of using it. The cumulative risk over time, however, is sufficiently great to justify more analysis of our key vulnerabilities.

It is important to note that the US intelligence community and Department of Defense is already addressing many of these issues, as is the National Security Council and a broader federal Homeland defense effort. At the same time, these are all areas where Congressional oversight can play a major role in assessing the quality of the intelligence effort and the broader effort within the Executive Branch.

Other Problems in Intelligence

Let me close with several comments focused on the problem of intelligence coverage of terrorism and asymmetric warfare. It has been some years since I was directly involved in intelligence planning and assessment, but there are some things that never seem to change:

- **It is far easier to call for strategic warning than to get it, or get policymakers to act on it of they do receive it**. We can always improve our analysis of warning indicators. In fact, the intelligence community does this all the time. We cannot, however, count on any method of analysis sorting through the constant "noise level" in these indicators and providing reliable probability analysis or warning. Furthermore, we cannot count on policymakers reacting.

  We should improve our analysis, but no system of warning, defense, and response can *rely* on strategic warning. Moreover, it is my impression that even when the intelligence community does make improvements, decision-makers choose to ignore unpopular or expensive warning or demand that the community free them from the burden of ambiguity and uncertainty.

  It is always easy for decision-makers to demand prophecy and attack intelligence analysis when they don't get it. This may explain why there are so many calls for improved strategic warning and so few calls for improved decision-maker response.

- **It is far easier to call for better HUMINT than it is to get it.** I have listened to three decades of calls for improved human intelligence. In practice, however, it remains as underfunded as ever, and partly because it is so difficult to make cost-effective investments and to be sure they pay off. Far too often, successes are matters of chance and not of the scale of effort.

  Yes, we should improve HUMINT – where we can show there is a feasible plan and a cost-effective path for success. However, calling for improved HUMINT all too often is both a confession of the severe limits of National Technical Means and a substitute for serious planning and effort.

- **New intelligence toys are not new systems, and systems always have limitations**. The other side of this coin is that we probably face growing limitations in our imagery and signals intelligence capabilities in many of the areas that affect our vulnerability to asymmetric warfare and terrorism. These are not a problem that should be addressed in open testimony, nor can I claim that my background in these issues is up-to-date. However, it is far from clear that some of the extremely expensive improvements we plan in National Technical Means will really pay off in the areas we are discussing today, or that some of the new tactical detectors and sensors being developed are integrated into effective systems. There may well be a need for independent net intelligence assessment of our probable future capabilities in these areas.

- **We need more focus on weaponization, weapons effects, and different kinds of vulnerability**. Proliferation and changes in information warfare are creating major new challenges in how the community should assess the weapons available to state and extremist actors. This is particularly true of biotechnology and information warfare, but it also involves the risk of "dirty," unsafe, and unpredictable nuclear weapons. Most weapons effects analysis is badly dated, and related to use against military targets. Weaponization analysis often does not address the acute uncertainty that may occur in weapons effects, and most vulnerability analysis is now dated. The technical issues of what attackers can really do, the problem intelligence may face in characterizing their resources, and the risk of combinations of new methods of attack – combining information systems and CBRN attacks, cocktails of biological weapons, etc. needs more attention.

- **We need an effective bridge between foreign intelligence and law enforcement that responds to the scale of the emergency.** We now have a wide range of barriers between foreign intelligence collection, surveillance of US citizens and activities within the US, military operations, and law enforcement activities. In general, these involve useful and necessary protections of American civil liberties. If, however, the threat rises to the level of a tangible risk an attack may use effective biological weapons, use nuclear weapons, or cripple our critical infrastructure, we need some way to react to a true national emergency that eliminates as many of these barriers as possible, and which does so at the state and local level and not just the federal one. We have long talked about the need for the "fusion" of intelligence and operations in warfighting. We may well face a similar need in Homeland defense, and the "fusion" of foreign intelligence and law enforcement activity will be critical.

One final point. Whenever new threats emerge, there is a natural tendency to call for new organizations, czars, and interagency structures. It is far easier to say that a new organization is needed than to get into the nitty gritty of actually having to improve existing capabilities or develop new ones. A set of problems involving this many uncertainties and new skills may or may not require new federal organizations, and new organizations within the intelligence community,

Ultimately, however, what improving our capability to deal with terrorism and asymmetric warfare requires most is resources and improving collection, analysis, and fusion at sophisticated technical levels. The real issue is one of how to improve depth, give the community the right perspective, and how to improve "quality," and not how to change organization or leadership. This requires both serious planning and a serious program and supporting budget. Changing the name on the door is almost mindlessly easy, but changing the capability within is what counts.